

SECURITY GAP ANALYSIS & AUDIT REPORTS

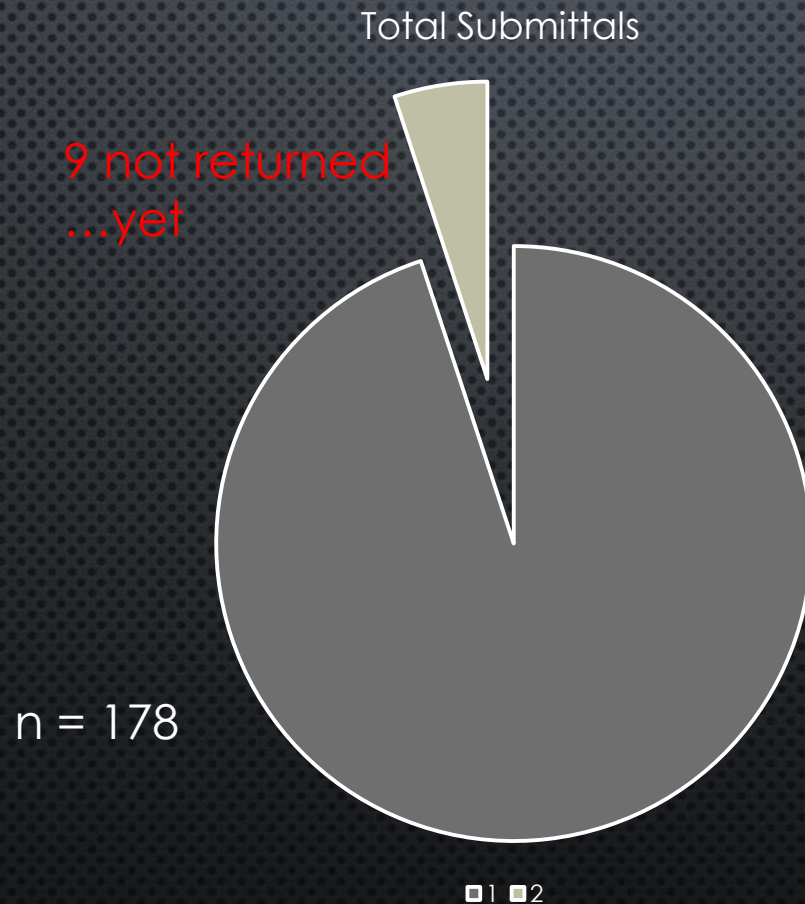
TAC UPDATE – DECEMBER 9, 2016

STEWART BRUNER

&

RICHARD BLAIR

TOTAL RETURNS TO DATE – 95%



MISSING COURTS / DEPTS.

- BISBEE MUNI & JUSTICE
- PIMA (GRAHAM) MUNI
- MAMMOTH JUSTICE
- MARICOPA (PINAL) JUSTICE
- AVONDALE MUNI
- FLORENCE MUNI
- YUMA ADULT PROBATION
- FOUNTAIN HILLS MUNI

CHARACTERIZING COURTS' SECURITY

ONE-TIME, CATCH-UP STATUS

- MINIMUM SECURITY STANDARDS TABLE
COMPARISON EFFORT 7/1 TO 9/30

ONGOING SECURITY TRENDS

- NETWORK SCANS / AUDIT REPORTS 2X
PER YEAR MINIMUM (PER 4.14)

Cyber Subcommittee Report to COT at Annual Meeting

DOCUMENTED GAPS / NON-COMPLIANCE



GAP-RELATED ACTIVITIES

- 10/24 INITIAL REVIEW. DECISIONS, AND REQUESTS FOR CLARIFICATION
- STAFF COMMUNICATED DECISIONS AND REQUESTS BACK TO COURTS
- 12/1 FOLLOW-UP MEETING – 12 GAPS AT 5 COURTS
- CALLS TO CITIES STILL REQUIRING CLARIFICATION, ESP. ON FIREWALLS
- ALL ACTION PLANS BEING MONITORED TO GIVEN DATES
- UPDATE AT NEXT MEETING IN JAN 2017

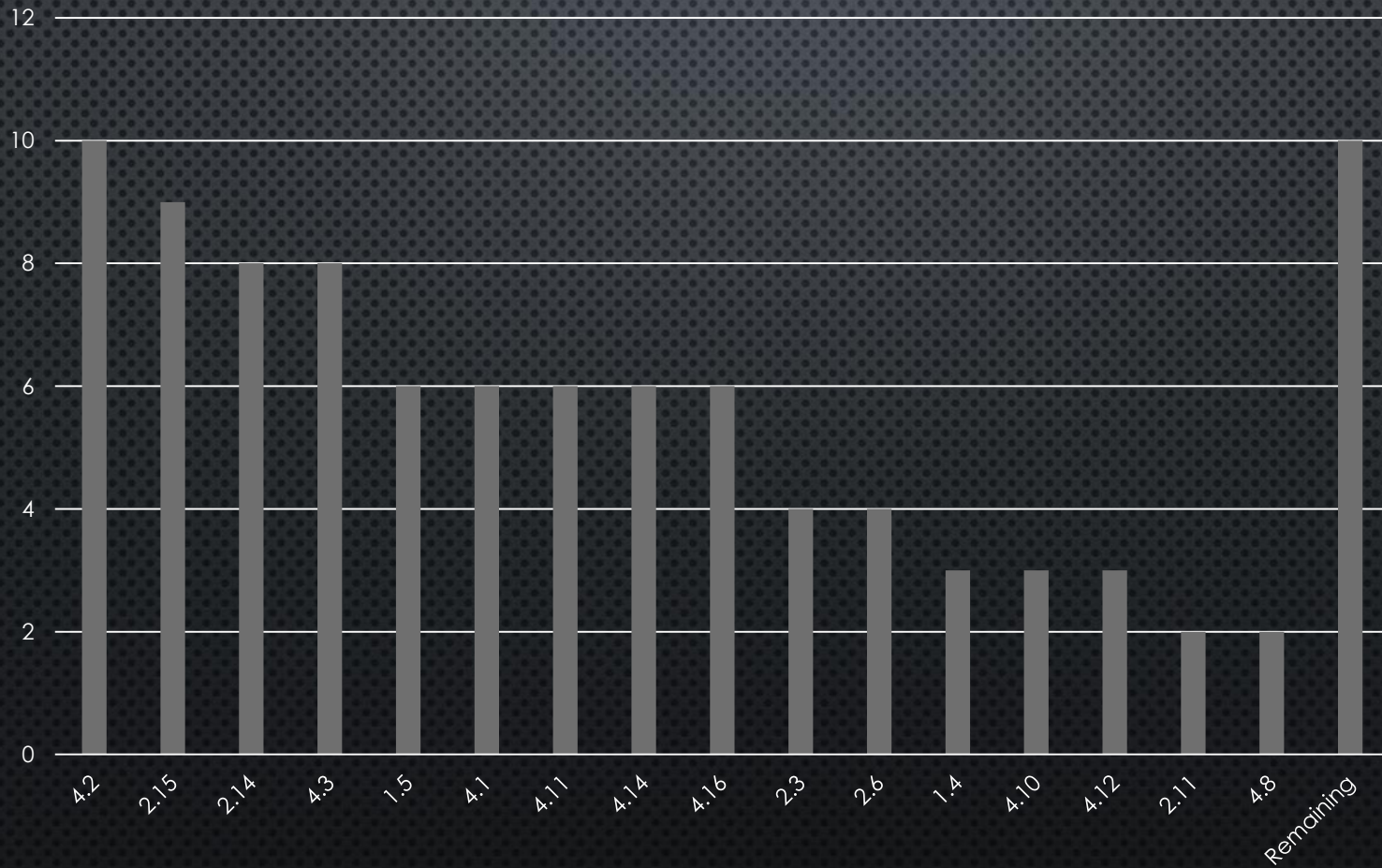
CONCERN ABOUT COURT FIREWALLS (ITEM 3.2)

3.2 – USER-BASED COMMUNICATION ACCESS BETWEEN COURT NETWORK USERS AND EXTERNAL RESOURCE ENVIRONMENTS OCCURS ONLY BY DIRECT ACCESS THROUGH A COURT FIREWALL. THIS MAY ALSO INCLUDE A ONE-WAY DOMAIN TRUST FOR USER AUTHENTICATION.

ISSUE – “COURT FIREWALL” IS SUPPOSED TO PROTECT COURT FROM OTHER CITY/COUNTY DEPARTMENTS ON INTERNAL NETWORK, NOT JUST FROM INTERNET

STAFF CONCERN – ALL BUT ONE NON-AJIN RESPONSES ARE “COMPLIES” YET CALLS TO INDIVIDUAL COURTS INDICATE NO FIREWALL EXISTS BETWEEN THE COURT AND OTHER CITY DEPARTMENTS – ALL ARE ON THE VERY SAME NETWORK DOMAIN.

FOLLOW-UP ITEMS FOR 12/31 ONLY



FOLLOWUP-RELATED ACTIVITIES

- STAFF REVIEWED AS RECEIVED AND BEGAN TRACKING
- 12/5 REMINDER E-MAIL SENT (FROM KAT)
- E-MAILS AND UPDATED TABLES BEING RETURNED NOW
- ITEMS NOT COMPLETE BY 12/31 REQUIRE ACTION PLAN
- ACTION PLANS REVIEW AT NEXT MEETING IN JAN 2017

AUDIT REPORT DETAILS

- SEC STD 4.14 REQUIRES 2X / YEAR AUDIT OF NETWORK ATTACHED ITEMS
- AOC SCANNED AJIN 7/10/16 THRU 8/29/16
- PRODUCED STANDARD REPORTS BY COUNTY W/ BACKUP MATERIALS
 - 3 AREAS SUMMARIZED
 - 3 CATEGORIES OF CRITICALITY
- ALL REPORTS RETURNED TO COUNTIES
- HIGH CRITICALITY ITEMS REQUIRE 90 DAY REMEDIATION
 - NON-CRITICAL REQUIRE TIMELINE FOR REMEDIATION
 - CAN REQUEST INTERIM SCANS TO REVIEW PROGRESS
- WILL SHARE LEARNINGS WITH COT CYBER SUBCOMMITTEE
 - TRACK OVERALL TRENDS AND BY INDIVIDUAL COURT OVER TIME

NEXT STEPS

- REMINDED NON-AJIN COURTS OF 4.14 2X/YEAR SCAN REQUIREMENT
 - RECEIVE INITIAL REPORTS AND PLANS IN MARCH
- RESPONDING TO QUESTIONS AND CLARIFICATION REQUESTS FROM AJIN COURTS
 - REMIND OF 90-DAY REQUIREMENT ON HIGH VULNERABILITY ITEMS
- REVIEW ALL PLANS FOR ADDRESSING HIGHEST VULNERABILITY ITEMS
- TRACK NUMBERS OF VULNERABILITIES BY CATEGORY BY COURT
- UPDATE SUBCOMMITTEE IN JANUARY AND EARLY MAY
 - CREATE PUBLIC MEETING REPORT FOR COT 6/1/17 W/ POSS EXEC SESSION
 - INCLUDE BOTH AJIN AND NON-AJIN RESULTS